wBefore the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the	)	CC Docket No. 96-115
Telecommunications Act of 1996:	)	
	)	
Telecommunications Carriers' Use of	)	
Customer Proprietary network	)	
Information and other Customer	)	
Information;	)	
	)	RM-11277
Petition for Rulemaking to Enhance	)	
Security and Authentication Standards	)	
for Access to Customer Proprietary		
Network Information		

Comments of the Public Utilities Commission of Ohio

Introduction

On February 14, 2006, the Federal Communications Commission ("Commission" or "FCC"), in response to a petition filed by the Electronic Privacy Information Center ("EPIC") released a Notice of Proposed Rulemaking ("NPRM") seeking comment on what, if any, additional steps the Commission should take to further the protection of customer proprietary network information[1] ("CPNI") that is collected and held by

---

[1] Customer proprietary network information or CPNI is defined in 47 U.S.C. § 222 (h)(1) as "(a) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (b) information contained

Footnote continued on next page.

telecommunications service providers.[2] Recognizing the threat to customer safety and security posed by breaches in the privacy protection afforded to CPNI, the Public Utilities Commission of Ohio ("Ohio Commission") applauds the Commission's efforts to reexamine the issues of CPNI privacy protection and appreciates the opportunity afforded by the Commission to provide comment for its consideration as it leads a response to this growing problem.

In recent weeks, the issue of protecting the privacy of CPNI from unscrupulous online data brokers has come to the forefront of the public discourse concerning privacy protection. The problem that has emerged is that CPNI has become a valuable marketplace commodity and is subject to threats that were nonexistent at the time the Commission adopted its current CPNI rules. Consequently, as more is learned about the ability of these data brokers to obtain and disseminate CPNI in a matter of a few hours, the need to ensure the privacy of CPNI and, consequently, to revisit current CPNI privacy regulations has taken on new importance. Section 222(c)(2) of the Telecommunications Act strongly implies that CPNI is to be disclosed only

---

Footnote continued from previous page.

in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

[2] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Consumer Proprietary Information and other Customer Information; Petition for Rulemaking to Enhance Security and Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, (rel. Feb. 14, 2006) (hereinafter "*NPRM*") [71 Federal Register 13317 (March 15, 2006)].

with the verifiable approval or initiation of the customer.[3] To preserve the intent of Section 222, the Ohio Commission recommends that the Commission modify its current CPNI rules to mitigate the present-day threats to the privacy of CPNI and take extra care in designing revised CPNI rules to ensure that CPNI is released only at the verifiable request or approval of customers.

The vulnerability of CPNI to unauthorized access by third parties through methods such as "pretexting"[4] has reduced the effectiveness of the "customer approval" mechanisms found in the Commission's current CPNI rules[5] as well as the effectiveness of many carriers' CPNI protection policies and practices. While the CPNI rules effectively protected customers' privacy in simpler times, those provisions are not proving to be adequate in today's connected world due to the increased commercial value of customers' personal information. The FCC's CPNI rules must protect customers' privacy today as effectively as they did in the past when there were considerably fewer threats to security.

The comments received from the industry in response to the Commission's NPRM will certainly shed light on the methods

---

[3] *See* 47 U.S.C. § 222.

[4] "Pretexting" is defined as "the practice of pretending to have authority to access protected records." Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115, 1 (filed Aug. 30, 2005) (hereinafter "EPIC Petition").

[5] *See* 47 C.F.R. § 64.2007.

telecommunications service providers use to protect CPNI; however, the Ohio Commission is concerned that the Commission may not receive all of the information that is required to adequately address this issue through a public forum such as a request for comments. In the NPRM, the Commission has asked questions[6], which, if honestly and accurately answered by the industry, may pose legitimate concerns for those responding to the Commission's queries. The Ohio Commission believes that the questions posed by the Commission are questions that must be asked and honestly and accurately answered to fully understand and address the issue of protecting CPNI privacy. However, concerns over liability for breaches which have occurred, increased vulnerability and targeting if successful exploits become public, and interference with internal investigations and responses may inhibit telecommunications service providers from providing full and complete responses. Consequently, the Commission may not receive all of the information needed. The Commission recognized this possibility in the NPRM and suggests that telecommunications service providers with such concerns develop anti-fraud tactics away from public scrutiny through

[6] As examples, the Commission asked how data brokers are able to obtain CPNI from telecommunications service providers; how CPNI is being made available to unauthorized third parties; the extent to which third parties are able to obtain unauthorized access to CPNI; the methods by which third parties obtain access to CPNI; whether there is evidence that third parties are "hacking" or otherwise obtaining unauthorized access to CPNI; if there is evidence of hacking, if there is evidence that it is widespread; whether there is evidence that dishonest insiders are providing unauthorized access to CPNI to third parties; what the current practices of telecommunications service providers regarding the disclosure of CPNI are and whether they are sufficient; and the methods used to transmit and provide CPNI. *NPRM* at ¶¶ 11 and 13.

alternate methods such as employing a working group to address the issue.[7] In addition to such alternatives, the Ohio Commission, in an effort to ensure that the FCC receives full and complete responses to its questions, encourages the FCC to consider alternate forums in which telecommunication service providers may respond to the Commission's queries, yet be assured that their interests are protected.[8]

The Ohio Commission recognizes that much of the information sought by the Commission in the NPRM is best supplied by those in the telecommunications industry itself. Consequently, the Ohio Commission will focus on the proposals raised by EPIC in its petition as well as those queries that are of such nature that the Ohio Commission can provide meaningful substantive comment.

---

7 *See NPRM* at ¶25.

8 As an example, the Commission could meet with members of the industry through *ex parte* discussions in which the meeting and topic are disclosed in compliance with the meet and disclose requirements, yet the detailed substance would remain confidential.

Ohio Commission Comments on EPIC Proposed Security Measures

While it is clear that a threat to personal privacy through the unauthorized access to CPNI exists, and is described in the EPIC petition[9], the nature of that threat (the means by which the information is obtained) is uncertain. In its petition, EPIC mentions three categories of threats: pretexting, electronic security failures, and insider action.[10] Each of these three types of threat demands a different response. Since there is no clear indication of the method (or predominant method) used to obtain the information, a "shotgun" approach, which responds to all 3 methods, seems reasonable. As such, EPIC has set forth five proposed security measures that it believes, if implemented, will better protect CPNI. These security measures are customer set passwords, audit trails, encryption, limitation of data retention, and notice.[11]

EPIC's proposed security measures can, for purposes of these comments, be divided into three broad categories: those that impart more customer-control; those that "raise the hurdle"; and those that pertain to enforcement.

Customer Control Security Measures

9 *See, e.g.*, EPIC Petition at 3-4.
10 *See id.* at 1.
11 *Id.* at 5-6.

These security measures will give customers a greater control over the release of their CPNI. Of the EPIC proposed security measures, customer-set passwords and notice fall into this category.

Customer-set Passwords

In its NPRM, the Commission asks for comment on the advisability of requiring telecommunications service providers to adopt a customer set password system to protect access to customers' accounts and their CPNI.[12] Furthermore, the Commission asks how customer-set passwords can be implemented so that, for example, data brokers engaged in pretexting would be most effectively barred from accessing CPNI.[13]

Passwords are used extensively to conduct online transactions with banks, credit unions, financial services, educational institutions, and for numerous other online services. They are used widely for online and offline retail stores, auctions, and subscription services. The Ohio Commission believes that a customer-set password requirement should be considered for the protection of CPNI.

A customer-set password has the effect of protecting customers in two ways. First, it acts as a safeguard against the release of personally identifiable CPNI. The quality of this protection is directly proportional to the quality of the password chosen by a customer, which puts the control of the effectiveness of this particular safeguard in the hands of the customer. The second way in which customer set passwords protect customers is that such passwords remove the need to have bibliographic information as an

12 *NPRM* at ¶ 16.
13 *See id.*

identifier of the customer. This is an improvement over the current system simply because verification of bibliographic information such as social security numbers or birthdates requires that this information be retained by telecommunications service providers in such a manner as to allow customer service representatives' ready access. Since the bibliographic information is itself useful for a number of inappropriate and illegal activities (such as identity theft), the use of bibliographic information to prevent a loss of privacy itself poses a risk of loss of privacy (of the biographic information). The implementation of customer-set passwords would help protect against both of these potential losses of private information.

As noted, the quality of the protection provided by customer-set passwords (or indeed by any password) is directly proportional to the quality of the password and the quality of its protection. An easily guessed (or obtained) password is of little more benefit than no password at all. Furthermore, there is a chance of customers forgetting their passwords. In most cases, however, this problem can be adequately handled through the use of "shared secrets" between the customer and the telecommunications provider. Finally, and perhaps most importantly, customer-set passwords, like any password, are vulnerable to pretexting of customers similar to the "phishing" schemes currently common in e-mail sent to obtain passwords and other information particularly in the financial sector.

It is also true that passwords may "hamper the transaction of legitimate business." The risk of "hampering", though, must be balanced with the risk customers are exposed to when they do not use a password. In a customer-set password system, customers must be given notice that the failure to use a secure password could expose their CPNI to illegitimate access and other negative consequences. To overcome fraudulent access to a password, the Ohio Commission agrees that using "shared secrets"[14] as well as providing notice to customers through telephone or internet notification when their passwords have been changed, would be an effective strategy for protecting CPNI in a customer-set password system. Consequently, the Ohio Commission recommends that the Commission adopt a customer-set password requirement in any rules adopted to further protect CPNI.

Notice

EPIC proposes a requirement that telecommunications service providers provide customer notice, similar to that which, unfortunately, has become commonplace in the financial industry, when the security of CPNI has been breached. The Commission, in its NPRM, invites comment on the

[14] "Shared secrets" include information not available from public sources such as the name of a pet or the make and model of one's first automobile. *See NPRM* at ¶ 15 citing *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Consumer Proprietary Information and other Customer Information; Petition for Rulemaking to Enhance Security and Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Information* , CC Docket No. 96-115, Reply Comments, 5 (November 9, 2005) (hereinafter "EPIC Reply Comments").

potential value of notification as a precautionary measure before releasing CPNI.[15]

The Ohio Commission agrees that customers should be given notice if the security of their CPNI has been breached. The benefit of such a "post breach" notice requirement is to provide customers with the knowledge that their privacy has, in fact, been breached, and to put within their control the ability to take steps to mitigate the personal risk from the breach. In order to notify customers of a breach, however, the telecommunications provider must be aware of the breach. As has been demonstrated in the financial industry, this "after-the-fact" notice, in the case of electronic security breaches, can be a case of "too little, too late". In addition, if CPNI is fraudulently obtained through pretexting, there may be no indication that there was ever a breach.

While the requirement to notify the customer when the security of CPNI has been breached is an obvious first step, for customer notice to be truly effective, customers must be given notice whenever there has been access to their CPNI, not merely after a breach has been discovered. Such notice would protect customers in three ways. First, customers would have confirmation of the release of CPNI if such release was legitimate. Second, customers would have earlier notice of the release of CPNI if such release was not legitimate. In other words, customers would be able to detect when their CPNI has been accessed through pretexting or some other inappropriate

---

[15] *Id.* at ¶ 22.

means. Third, the telecommunications service provider would have confirmation that the release of CPNI was (or was not) legitimate. Notice such as this would provide telecommunications service providers a diagnostic tool to aid in determining who has breached a customer's CPNI privacy, when the breach occurred, and how the breach occurred. Such notice could be accomplished through a simple requirement that telecommunications service providers call a customer at a known legitimate telephone number to confirm the release of CPNI, through the mail sent to the customer's billing address, or through an e-mail sent to the customer's known e-mail address.

The Commission also asks what would be the value of notifying customers prior to releasing CPNI by calling the customer's registered telephone number for the customer's account to verify the identity of the customer prior to releasing CPNI to the customer.[16] By giving customers notice prior to releasing CPNI, telecommunications service providers would add a significant layer of additional protection to CPNI privacy, although at some cost and hindrance to the marketing efforts of the telecommunications service provider. This may be a preferable option compared with the proposal for notice described above because the verification is performed using the customer's own telephone line of record at the residence or business of the customer or to the customer's e-mail address. It would be difficult for those

16 *Id.*

engaged in pretexting or other unauthorized persons to access a customer's CPNI with such a security system.

Security Measures that Raise the Hurdle

No security system (that actually allows legitimate access) is perfect. If there is a legitimate way to access the information, there is going to be a less than legitimate way to access the information. A locked door can be opened with either a key or a lockpick. To prevent such illegitimate means of access, the degree of difficulty of access can be raised and/or the value of the information can be lowered so that the incentive to access the information for illegitimate reasons is reduced below a practical level. EPIC's proposals to require encryption and limit data retention have the effect of "raising the hurdle" in this manner.

Encryption

EPIC recommends that telecommunications service providers store data in an encrypted form.[17] The Commission asks commenters to discuss the usefulness of encryption and to weigh the costs and benefits of encryption.[18]

Encryption provides some degree of protection since it increases the difficulty of obtaining anything useful from access to the data. However, encryption may be of limited practical use, since the information must be decrypted at some point within the carrier's computer systems (such as when generating customer bills and statements). If the decryption process is on a computer system that is networked, it is open for attack. Encryption, though, has the effect of "raising the hurdle" in obtaining useful information from such an attack by narrowing the numbers and types of systems where the data is readily available. In addition to providing some protection to CPNI within a telecommunications service provider's network, encryption may also, and more importantly, provide CPNI protection in the event that storage disks or other data storage media are lost or stolen.

Limiting Data Retention

The Commission seeks comment on EPIC's proposal that CPNI records be deleted and asks when this should be done if, in fact, such records should

---

17 *See* EPIC Petition at 6.

18 *NPRM* at ¶ 19.

be deleted.[19] EPIC's proposal to limit data retention may have the effect of lowering the value of the information that is otherwise being obtained through illegitimate an unauthorized means. According to EPIC, some data-brokers offer service to retrieve telephone call records.[20] Some offer services to spouses to spy on each other from which one spouse may benefit from obtaining the other's CPNI.[21] Such CPNI is advertised as available and often provided in a matter of hours and implies that an official, legal means of obtaining CPNI, such as through a subpoena, is typically not used.[22] If telecommunications service providers limit the type of data that they retain, then the value of the data may, in fact, be of little use, depending on the type of data retained, and, consequently, of little value to data brokers. Limiting data in this manner, though, would also limit the legitimate uses (such as questioning charges) that customers may legitimately make of their own CPNI. Furthermore, if the length of time that data is retained is reduced without altering the threshold for the type of data that is retained, such limitation could have the undesired inverse effect of increasing the commercial value of CPNI (and therefore the lengths a data broker might go to obtain it) due to the smaller window of time in which it is available to be obtained.

---

19 *See id.* at ¶ 20.
20 EPIC Petition at 3.
21 *Id.*
22 *See id.* at 3-4.

In addition to limiting legitimate customer use of CPNI and actually increasing the value of CPNI, limiting data retention may also run afoul of data retention requirements. In Ohio, telecommunications service providers are required to maintain customer billing records for 18 months.[23] This retention period allows customers to request bill copies and question charges billed in prior months and appearing on

[23] O.A.C. 4901:1-5-15 (E).

statements which they may no longer have. This period of time also allows Ohio Commission staff a sufficient period of time to obtain customer billing records when investigating whether or not a telecommunications service provider is in compliance with the Ohio Commission's rules and regulations. Furthermore, regulations in Ohio set forth minimum requirements for what must appear on a customer bill.[24] This ensures that customers receive a bill that includes all of the information necessary to answer any questions about a particular month's charges.

In declining to support EPIC's proposal to limit data retention, the Ohio Commission wishes to note that the Commission's rules governing the retention of telephone toll records require that toll service providers maintain toll records for 18 months.[25] Such records include the name, address, and telephone number of the caller, telephone number called, and date, time and length of the call.[26] In addition to conflicting with state data retention requirements, the EPIC proposal to limit data retention, if adopted by the Commission, would likely conflict with the Commission's current data retention requirements.

As an alternative to deleting CPNI data records, EPIC suggests that telecommunications service providers should "de-identify" records. That is, they should separate identifying data from the general transaction record.

---

24 *See* O.A.C. 4901:1-5-15(A)(B)(C).

25 47 C.F.R. § 42.6

The Ohio Commission cautions against the Commission adopting any requirement that would frustrate customer efforts to raise billing disputes with their telecommunications service providers as well as

---

Footnote continued from previous page.

[26] *Id.*

the efforts of state regulators to investigate the account billing of any particular provider. Any requirement that the identity of a customer be separated from the general transaction record prior to the end of a state's required data retention period would do just that. EPIC recognizes that data records should not be deleted until they are no longer needed for billing or dispute settlement purposes. Likewise, customer identifying information should not be separated from the general transaction record until the record is no longer needed for these purposes.

Enforcement Security Measures

Audit Trails

The third type of security measure proposed by EPIC may be categorized as an enforcement measure. The implementation and use of audit trails falls into this category. In making its proposal, EPIC suggests that the Commission require telecommunications service providers to extend the rule found in §64.2009(c)[27], which requires telecommunications providers to record each instance of its, its affiliates', or its third party contractors' use of CPNI in their marketing campaigns.[28] This extension would require recording all access to a customer's records, including the date, information disclosed, and the person to whom the information was disclosed. The

[27] *See* 47 C.F.R. § 64.2009(e).
[28] *See* EPIC Reply Comments at 7.

Commission asks commenters for an assessment of the benefits and burdens of this requirement.[29]

Audit trails would provide a means of allowing telecommunications service providers to document those employees who have accessed CPNI and the times at which they did so. If employees with access to CPNI must identify themselves each time they retrieve CPNI and this is logged along with the time and information accessed, telecommunications service providers would have a means of tracing CPNI disclosure and better identifying the source of dissemination to third parties. In doing so, telecommunications service providers would be able to take appropriate action against rogue insiders who may supply CPNI to unauthorized third parties. Furthermore, if telecommunications service providers are required to maintain records sufficient to construct an audit trail of CPNI which has been accessed and disclosed, such information would be discoverable by the Commission and state commissions for purposes of taking enforcement action against any telecommunications service provider that is not adequately protecting CPNI.

While requiring records such that an audit of CPNI access may be constructed will help alleviate the problem of insiders disclosing CPNI to unauthorized third parties, the weakness of such a security measure is that, by itself, it will not prevent innocent disclosure to unauthorized third parties

---

[29] *NPRM* at ¶ 18.

engaged in pretexting. Combined with another security measure, such as a consumer-set password, which must be revealed by the caller to receive CPNI, the requirement of audit trails could provide additional protection for CPNI as well as an enforcement tool for both the telecommunications service providers to use internally and for regulators to use should the telecommunications service providers not be taking adequate steps to protect CPNI.

Recommendation on EPIC Proposals

The Ohio Commission believes that EPIC has proposed several security measures which warrant further consideration. None are sufficient to singularly address the CPNI privacy issue and each has advantages and disadvantages. In these comments, the Ohio Commission has endeavored to be balanced in its assessment of each proposal and, after careful consideration, encourages the Commission to consider incorporating customer-set passwords, appropriate notice, encryption, and audit trails into any CPNI privacy rules that it may promulgate. The Ohio Commission also sees some benefit in limiting data retention; however, when balanced against the disadvantages of such a requirement, the Ohio Commission encourages the Commission to reject limiting data retention inasmuch as such limitation would interfere with state data retention requirements. If either the type of information retained or the length of time that the information is retained is altered, the benefits afforded by data retention to customers as well as the

Ohio Commission's ability to fully and adequately investigate the billing practices of telecommunications service providers, both of which are provided for by Ohio's telephone billing requirements, will be compromised and perhaps lost altogether. The Ohio Commission suspects that similar results would occur in other states as well. For this reason, the Ohio Commission requests that the Commission carefully consider any rule limiting data retention and the effect that such a rule would have on both customers and state commissions' ability to adequately regulate in the area of telephone service billing.

The Commission asks what specific rule changes are needed to identify and solve the concerns raised by EPIC.[30] While any rules adopting the EPIC proposals must be sufficiently clear to set a baseline expectation of telecommunications service providers,

[30] *NPRM* at ¶ 13.

the Ohio Commission cautions the FCC about being too specific in the technical standard it adopts. When the technical requirements for the implementation of a rule are uniform, the benefits of a breach of this technical standard are greatly increased. If, for instance, a single universal system is required for the protection of CPNI, then the development of a single successful exploit would make all telecommunications service providers using this system vulnerable. The result would be an "arms race" between the telecommunications service providers and those wishing to exploit the system, with the advantage being to the latter since they do not need to obtain FCC approval for a change in approach. Consequently, the Ohio Commission encourages the FCC to adopt rules requiring telecommunications service providers to implement each of the EPIC security measures with the noted exception of the limitation on data retention; however, any rules adopted by the FCC should not be overly prescriptive in establishing technical standards or a specific methodology for compliance.

Additional Comments of the Ohio Commission Regarding CPNI

Many of the security measures proposed and set forth by EPIC, if adopted, will, in the opinion of the Ohio Commission, enhance the protection of CPNI. However, any preventative measure can be defeated with enough persistence. Taken together, though, the EPIC proposals endorsed by the Ohio Commission would provide an even more effective suite of countermeasures to protect the CPNI retained by telecommunications service

providers. Nonetheless, the Commission recognized that to develop rules that fully protect CPNI, additional questions beyond those pertaining to the EPIC proposals must be asked.

Limitations on the Transfer of CPNI

Transfer of CPNI Should be Limited to Opt-In Only Authorization

The Commission also asks whether there should be any limitation(s) on the transfer of CPNI. The Ohio Commission believes that there should be limitations beyond those found in the Commission's current CPNI rules. Under the Commission's current rules, CPNI can be disclosed and transferred to the third-party affiliates of telecommunications service providers for marketing purposes subject to "opt-in" or "opt-out" approval.[31] The Ohio Commission encourages the FCC to amend its CPNI rules such that they no longer include an "opt-out" approval process.[32] Customers wishing to receive marketing solicitations should have the opportunity to opt in to receiving such solicitations at the time they establish their service or, for existing customers, at the time that they are made aware of the new "opt-in only" regime, either through bill insert or voice response unit message (if calling the telecommunications service provider). Clearly, if the transfer of individually identifiable CPNI is limited, the likelihood of the unauthorized disclosure, abuse, or loss of customers' CPNI is correspondingly lessened.

The Impact of Section 222(c)(2) on the Transfer of CPNI

---

[31] *See* 47 C.F.R. § 64.2007.

[32] In advocating an "opt-in only" regime, the Ohio Commission supports reply comments filed by EPIC *et. al.* on November 16, 2001. *See In the Matter of Telecommunications Carriers' Use of Customer Proprietary Network Information*, Reply Comments of The Electronic Privacy Information Center *et. al.*, CC Docket Nos. 96-115, 96-149.

The Commission's NPRM raises the issue what impact Section 222(c)(2) has on the issue of the transfer of CPNI.[33] Section 222(c)(2) states that telecommunications service providers shall disclose CPNI upon affirmative written request by the customer,

[33] *NPRM* at ¶ 13.

to any person designated by the customer. Conversely, then, if the customer has not given affirmative written consent for disclosure to a third party, the telecommunications service provider shall not disclose CPNI to that third party. Section 222(c)(1) allows for the disclosure of CPNI, without the customer's affirmative written authorization, for the purpose of provisioning the service from which the CPNI is derived or is a service necessary to, or used in, the provisioning of such service. Section 222(c)(2), then requires the customer's affirmative written authorization for all other third-party disclosure.

The Ohio Commission does not believe that the marketing of communications-related services rises to the level of the exception granted in Section 222(c)(1) and, consequently encourages the FCC to amend its opt-in/opt-out approval regime such that it is consistent with the requirement of Section 222(c)(2). It should not matter whether the third-party is an affiliate or not or whether the purpose is to market the customer. If the customer has not provided a written affirmative consent for disclosure of CPNI, i.e., "opted-in", telecommunications service providers should not disclose a customer's CPNI. As stated above, each transfer of CPNI opens the door to potential breaches of CPNI privacy. Since the customer is the party most directly affected by a breach of his or her CPNI, the Ohio Commission believes that it should be within that customer's control to limit the risk of unauthorized CPNI disclosure. Consequently, as previously articulated, the Ohio

Commission encourages the FCC to abolish the "opt-out" approval for CPNI disclosure to third-party affiliates and institute an "opt-in only" requirement for those customers wishing to receive third party marketing solicitations.

Customer Education

In addition to the measures discussed above, the Ohio Commission recommends that the Commission consider enhanced requirements for customer education as a necessary component in any strategy to strengthen and improve the protection of CPNI. As a general matter, telecommunications service providers should inform their customers about the security measures implemented to protect their CPNI and their role in that system of protection. Furthermore, customers must know and understand the threats that put the privacy of their CPNI at risk. It is only with this full awareness that telecommunications service providers and customers can work together to use the systems and tools available to them to most effectively protect customers' CPNI privacy.

"Opt-Out" Regime

The Commission asks what changes to its rules, if any, are necessary to ensure that customers fully understand what personal records telecommunications service providers seek permission to use or disclose. Under the Commission's current CPNI rules, customers' CPNI may be shared with third-party affiliates of telecommunications service providers subject to opt-out approval.[34] In other words, customer authorization is presumed unless the customer affirmatively states that it is not. Ideally, the Commission would reverse the standard to that of an "opt-in" customer

authorization before telecommunications service providers share customers' CPNI with their third-party affiliates. In the absence of such a change in the standard of customer authorization, the Ohio Commission believes that customer education is imperative to empower customers

---

Footnote continued from previous page.

[34] *See* 47 C.F.R. § 64.2007(b)(1).

with information necessary to understand the ramifications of the present opt-out requirement. At a minimum, telecommunications providers should be required to annually provide customers a listing of the CPNI it retains and regularly shares with its third-party affiliates for marketing purposes and inform customers of the steps necessary to opt-out of having this information disclosed should they choose to do so.

Customer Education Regarding Security Measures

The Ohio Commission believes that to truly be effective, customers must be adequately educated concerning security measures within their control. As noted above, two of the EPIC proposals are "customer-controlled" in their nature. By definition, customer set passwords fall under the control of the customer setting the password. Consequently, customers must be educated as to the necessity of creating an effective and secure password. Should the Commission adopt EPIC's customer-set password proposal, telecommunications service providers must educate their customers on establishing secure passwords. Such education could be provided through a bill insert that informs customers of the need for a customer-set password to access CPNI or through a voice prompt given to the customer when he or she calls to access CPNI.

Should the Commission adopt EPIC's notice proposal, customers must also be educated as to what such notice means. If the notice required is strictly "after-the-fact" notice, customers must be educated as to the steps

they must take to adequately guard against identity theft. If the notice required pertains to any request to disclose CPNI, customers must be educated as to the potential consequences of allowing such disclosure. Without such proper education, notice to customers will often prove to be an ineffective security measure.

Conclusion

The Ohio Commission appreciates both the opportunity afforded by the FCC to provide its thoughts and recommendations on the issue of CPNI privacy as well as the leadership of the Commission to address this important privacy concern. In order to provide customers the level of protection intended by Section 222 of the Act, the Ohio Commission recommends adopting many of the security measures proposed by EPIC. Due to the important role state commissions must play in helping protect CPNI privacy, the Ohio Commission encourages the FCC to reject EPIC's data retention proposal, to the extent such a rule would preempt state record retention requirements, and any other proposal that would limit the ability of states to regulate in this area. The Ohio Commission believes that customers should ultimately be in charge of the disclosure of their CPNI and, consequently, encourages the Commission to require telecommunications service providers to obtain customer authorization prior to disclosing CPNI to *any* third-party. Finally, for any changes in CPNI privacy regulation to have their desired

effect, customers must be educated. Education must include informing customers not only of the potential threats to their privacy, but also informing them of ways in which they can protect themselves. Again, the Ohio Commission appreciates the

opportunity to comment on this important issue and respectfully submits these comments for the Commission's consideration.

Respectfully submitted,

Stephen A. Reilly
Assistant Attorney General
Public Utilities Section
180 E. Broad Street, 9th Floor
Columbus, OH 43215-3793
(614) 466.4396
Fax: (614) 644.8764